CLAIMS:

1. A record carrier (1) having a first area (3) storing information (data), which is at least partly stored in encrypted form (E_{AK}(data)), this part being called an asset (E_{AK}(data)), and which includes a first part of decryption information (HCK, E_{DNK}(HCK)), and the record carrier (1) further having a second area (4) storing a second part of decryption information (UCID), wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (E_{AK}(data)).

2. A record carrier (1) as claimed in claim 1, characterized in that the first (3) and second areas (4) comprise storage media of a different physical kind.

3. A record carrier (1) as claimed in claim 1, characterized in that the second area (4) comprises a chip (4') for providing the store of the second area (4).

4. A record carrier (1) as claimed in claim 1, characterized in that

- a symmetric method using a first cryptographic key, called an asset key (AK), is used for asset en- and decryption, and in that
- the asset key (AK) is stored in the second area (4) in an encrypted form, wherein for its encryption a symmetric encryption method has been used, this method employing a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used.

5. A record carrier (1) as claimed in claim 1,
characterized in that
- a third cryptographic key, called a hidden-channel key (HCK), serves in the asset decryption, and in that
- the hidden-channel key (HCK) is obtainable from the first part of decryption information (HCK, E_{DNK}(HCK)), in particular, that the hidden-channel key (HCK) coincides with the first part of decryption information (HCK) and that the first part of decryption information (HCK) is scrambled and/or encrypted within the information (data) stored in the first area (3).

6. A record carrier (1) as claimed in claim 3,
characterized in that
- the chip (4') is designed for storing a first counter (C_i), and
- the chip (4') is designed for allowing an reading and/or writing device read access to the first counter (C_i) but denying write access to it, and
- the chip (4') is designed for changing the value of the first counter (C_i) each time the second part of decryption information (UCID) is read by an reading and/or writing device, and
- the chip (4') is designed for storing a second counter (C_e) in an encrypted form, wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the second counter (C_e).

7. A record carrier (1) as claimed in claim 3,
characterized in that
the chip (4') is designed for checking the right of an reading and/or writing device to access the record carrier (1).

8. A record carrier (1) as claimed in claim 1, characterized in that the second area (4) is designed for storing user-specific settings serving in controlling the access of an reading and/or writing device to the record carrier (1) and/or in controlling the manner information being read from the record carrier (1) is presented by the reading and/or writing device to a user of the reading and/or writing device.

9. A device for reading from and/or writing to a record carrier (1) as claimed in claim 1, wherein the device is designed

- for reading and/or writing the first part of decryption information (HCK, $E_{DNK}(HCK)$),
- for reading and/or writing the second part of decryption information (UCID),
- for reading and/or writing the asset ($E_{AK}(data)$),
- optionally, for obtaining complete decryption information from both the first (HCK, $E_{DNK}(HCK)$) and second parts (UCID) of decryption information, and,
- optionally, for decrypting and/or encrypting the asset ($E_{AK}(data)$) with the complete decryption information.

10. A device for reading and/or writing as claimed in claim 9, characterized in that

- the device is designed for accessing the first (3) and second areas (4) of the record carrier (1) in parallel.

11. A device for reading and/or writing as claimed in claim 9, characterized in that

- the device is designed for storing and maintaining a revocation list of identifiers (UCID), and in that
- the device is designed for at least partly refusing a user of the device access to a record carrier (1) as claimed in claim 3 if the identifier (UCID) being stored on the record carrier (1) belongs to the revocation list.

12. A system for supporting copy protection, the system comprising a device as claimed in claim 9 and a record carrier (1) as claimed in claim 1.

13. A method for reading from and/or writing to a record carrier (1) as claimed in claim 1, with the steps:

- reading and/or writing the first part of decryption information (HCK, E_{DNK}(HCK)),
- reading and/or writing the second part of decryption information (UCID),
- reading and/or writing the asset (E_{AK}(data)),
- optionally, obtaining complete decryption information from both the first (HCK, E_{DNK}(HCK)) and second parts (UCID) of decryption information, and,
- optionally, decrypting and/or encrypting the asset (E_{AK}(data)) with the complete decryption information.

14. A method for producing a record carrier (1) as claimed in claim 1, with the steps:

- selecting an identifier (UCID), in particular, selecting an identifier (UCID) being different from the identifiers (UCID) having previously been selected in the method,
- constructing the second part of decryption information (UCID) as comprising the identifier (UCID), and
- producing the record carrier (1) with the thus constructed second part of decryption information (UCID) being stored on the second area (4) of the record carrier (1).